
ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

PREAMBLE.

Freedom of expression and an open environment to pursue scholarly inquiry and for sharing of information are encouraged and supported at Loyola Marymount University. These values lie at the core of our academic community. While some computing resources may be dedicated to specific research, teaching, or administrative tasks that would limit their use, freedom of expression must, in general, be protected. The University's policy of freedom of expression applies to computing resources.

With free expression are certain personal obligations of each member of the LMU community to use computing resources responsibly, ethically, and in a manner that is in accord with the law and the rights of others. The campus depends first upon a spirit of mutual respect and cooperation to create and maintain an open community of responsible users.

As an institution of higher education, the University encourages, supports, and protects First Amendment rights and an open environment to pursue scholarly inquiry and to share information. Access to networked computer information in general and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. As with any resource, it is possible to misuse computing resources and facilities and to abuse access to the Internet. By using University information technology facilities and resources, users agree to abide by all related University policies and procedures, as well as applicable federal, state, and local law. Violations may result in University disciplinary action or referral to appropriate external authorities.

Computing resources are provided to support the academic research, instructional, and administrative objectives of the university. These resources are extended for the sole use of University faculty, staff, students, and other authorized users to accomplish tasks related to the user's status at the university, and consistent with the University's mission.

SCOPE OF POLICY.

This acceptable use policy applies to all users of University Information Technology Resources. This includes the resources under the management or control of Information Technology Services (ITS) or other units of Loyola Marymount University Excluding Loyola Law School. A "user" is defined as any individual who uses, logs into, or attempts to use or log into, a system; or who connects to, or attempts to connect to or traverse a network, whether by

hardware or software or both, whether on campus or from remote locations. The term "user" thus includes system sponsors and system managers, faculty, staff, students, and other customers. "Information technology resources" are those facilities, technologies, and information resources required to accomplish information processing, storage, and communication, whether individually controlled or shared, stand-alone or networked. Included in this definition are all information technology centers (e.g., departmental labs, classroom technologies, electronic resources, and computing and electronic communication devices and services, such as, but not limited to, computers, printers, modems, e-mail, fax transmissions, video, multi-media, instructional materials, and administrative systems). Personal equipment physically connected to the University network is also subject to this policy. This includes any technology already in place or to be deployed.

SECURITY AND PRIVACY.

The same principles of academic freedom and privacy that have long been applicable to written and spoken communications in the University community apply also to electronic information. The University cherishes the diversity of perspectives represented on this campus and, accordingly, does not condone either censorship or the casual inspection of electronic files such as but not limited to e-mail messages.

The University employs various measures to protect the security of its computing resources and of its user accounts. Users should be aware, however, that the University cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing passwords regularly. Users are responsible for maintaining backup and recovery systems in accordance with disaster recovery guidelines, as well as for implementing and maintaining computer security in accordance with best practices and University policies and procedures. The University respects encryption rights on its networks and may itself encrypt information and transactions when secure confidentiality is an obligation.

Users should also be aware that their uses of University computing resources are not completely private. While the University does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the University's computing resources require the backup of data and communication records, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service. The University may also inspect files or monitor usage for a limited time when there is probable cause to believe a user has violated this policy. Inspections or monitoring related to violations of this policy must be authorized in advance by the area vice president, in consultation with University counsel. Such inspections or monitoring will be conducted with notice to the user, unless, after consultation with University counsel, it is determined that notice would seriously jeopardize substantial interests of the University or of third parties. In addition, a supervisor or principal investigator may find it necessary to retrieve a file of assigned work by inspection without notice when an employee is unavailable for timely consultation.

In addition, users should be aware that their right to privacy in electronic records may be subject to the University's obligation to respond to subpoenas or other court orders, reasonable discovery requests, and requests for documents pursuant to the California Code.

University administrative records are subject to public record requests, unless an express exception recognizes the confidentiality of the material, such as the exception for library records. By statute, public records include all "records, documents, tape or other information, stored or preserved in any medium," whether generated by University administrators, faculty, or staff. The statute contains no express exception for documents generated by faculty or staff in the course of their employment. Although it is the University's position that personal electronic files of faculty, staff, and students are not ordinarily to be considered "public records," users should be aware that a court of law, and not University officials, may ultimately decide such issues, e.g., FERPA.

INDIVIDUAL RESPONSIBILITIES.

a. Use Resources Appropriately. Uses that interfere with the proper functioning of the University's information technology resources are prohibited. Such inappropriate uses would include but are not limited to insertions of viruses into computer systems, tapping a network or running a "sniffer" program, e-mail spam, chain letters, destruction of another's files, use of software tools that attack IT resources, violation of security standards, and the like.

b. Respect the rights of others. Interference with the ability of other users to make appropriate use of the resources is prohibited. Such inappropriate uses include, without limitation, invading the privacy of another's files or otherwise gaining unauthorized access to the files of another. Such uses would include but are not limited to denial of service attacks, misrepresentation, forgery, use of software tools that attack IT resources, and the like.

c. Adhere to the EDUCAUSE Code of Software and Intellectual Rights. The EDUCAUSE Code follows:

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

d. Adhere to data access policies. Accessing restricted data without permission or need to know is prohibited. Where access to restricted data is permitted, use of such data shall be limited to the purpose for which access was authorized. Secondary use of University data subject to access restriction, without adhering to the restrictions, is also not permitted.

e. Adhere to software licenses. Persons loading software on any University computer must adhere to all licensing requirements for the software. Except where allowed by University site licenses, copying software licensed for University use for personal use is a violation of this policy. Users are responsible for adhering to agreements for databases licensed by the University. Individual departments are charged with the

responsibility of ensuring that licensing requirements are met and for developing a statement guiding the installation of personal software on departmental computers.

f. Avoid Abuse of Resources. Personal use of computer resources should be kept to a minimum. Personal use may be abusive if it takes place during regularly scheduled work time, if it overburdens a network, if it results in substantial use of system capacity, or if it otherwise subjects the institution to increased operating costs. Division leadership will provide more specific guidance by formulating unit policies or providing advice on a case-by-case basis.

g. Prohibited Activities. Information technology resources, including the University's electronic address (e-mail, web), shall not be used for personal commercial gain, for charitable solicitations unless these are authorized by the appropriate University officer, for personal political activities such as campaigning for candidates for public office, or for lobbying of public officials. For purposes of this policy, "lobbying" does not include individual faculty or staff sharing information or opinions with public officials on matters of policy within their areas of expertise. Faculty and staff consulting that is in conformity with University guidelines is permissible.

h. Use University name as authorized. Unless authorized to speak for the University, users should avoid creating the impression they are doing so. Electronic exchange of ideas is encouraged. However, users shall take appropriate steps to avoid the possible inference that communication of a message via the University e-mail system or posting to an electronic forum connotes official University authorization or endorsement of the message.

i. Adhere to other University policies. Inappropriate use of electronic technology resources could violate applicable state, & federal laws, and University policies, including, without limitation, University policies on professional ethics and academic responsibilities, telephone procedures, intellectual property rights, human rights, against sexual harassment, violence or funds solicitation.

j. Obey external laws. Information technology resources shall not be used in a manner that violates federal, state, or local law, including without limitation the federal requirement that the University provide employment and educational environments free from race-based or gender-based hostility (see Titles VI and VII, Civil Rights Act of 1964, and Title IX, Educational Amendments of 1972); and state criminal laws forbidding harassment (IC 708.7), exhibition of obscene materials to minors (IC 728.2), rental or sale of hard core pornography (IC 728.4), official misconduct (IC 721), computer crime (IC 716A), and federal and state copyright and fair use laws. Nothing in this policy prohibits the use of appropriate material for educational purposes in any accredited school, or the library, or in any educational program in which a minor is participating. Nothing in this policy prohibits the presence of minors at an exhibition or display or the use of any materials in the library.

ADMINISTRATION AND ENFORCEMENT.

The Information Technology Governance committees are charged with the development, approval, and communication of IT policies. Requests for interpretation of this policy as applied to particular situations may be directed to the Vice President for Administration, who

will coordinate interpretation discussions with the IT governance committees and communication with the inquiring party.

Reports of apparent violations of the policy may be made to the Vice President for Administration, Information Technology Services, to an employee's supervisor or, in the case of a student, to the Office of the Vice President for Student Affairs. Where violations of law are alleged, University Public Safety should be contacted. Good faith disclosures of University-related misconduct are protected by the anti-retaliation policy. In most instances, concerns of possible violations of this policy will be addressed informally by discussion or admonition. Where sanctions are appropriate, they may include a formal reprimand, loss of user privileges for a definite or indefinite period, termination of employment, or, in the case of a student, probation, suspension, or expulsion from the University.

Serious or repeated violation of this policy by faculty members will be governed by the Faculty Handbook Procedures. Violations of this policy by staff members will be addressed by the Staff Handbook. Violations of this policy by students will be governed by the Judicial Procedures for alleged violations of the Code of Student Life/Conduct.

DISCLAIMER.

The University makes no warranties of any kind, whether expressed or implied, with respect to the information technology resources it provides. The University will not be responsible for damages resulting from the use of communication facilities and services, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a University employee, or by the user's error or omissions. Use of any information obtained via the Internet is at the user's risk. The University specifically denies any responsibility for the accuracy or quality of information obtained through its electronic communication facilities and services, except material represented as an official University record.

OTHER POLICIES AND RULES.

Users are advised that network traffic exiting the University is subject to the acceptable use policies of our national and international network connectivity providers or long distance communication providers.

January 16, 2003